Citation /

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-123759
(43)Date of publication of application : 17.05.1996

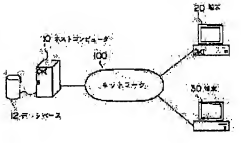
(51)Int.Cl. G06F 15/00
G09C 1/00

(21)Application number : 06-263934
(22)Date of filing : 27.10.1994

(71)Applicant : OKI ELECTRIC IND CO LTD
(72)Inventor : IWANO MASAHIRO
IWASAKI KENJI

(54) SECRET PROTECTION SYSTEM BASED UPON DATA EXCHANGE USING RANDOM NUMBERS

(57)Abstract:
PURPOSE: To provide a secret protection system attained by data exchange using random numbers and capable of preventing the occurrence of illegal access to a host computer.
CONSTITUTION: In the case of outputting a connection request from a terminal 20 to the host computer 10, the terminal 20 transmits user ID to the computer 10. At the time of receiving the user ID, the computer 10 transmits prescribed data to the terminal 20 to execute arithmetic processing based upon the prescribed data. At the time of receiving the prescribed data from the computer 10, the terminal 20 executes prescribed arithmetic processing based upon the data and transmits data including the arithmetic result to the computer 10 as a password. The computer 10 collates the data arithmetically processed based upon the prescribed data with the password received from the terminal 20, and when matched with each other, the computer 10 receives the connection request from the terminal 20.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平8－123759

(43)公開日　平成８年(1996)５月17日

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ｂ	9364－5L		
Ｇ０９Ｃ　1/00		7259－5J		

審査請求　未請求　請求項の数4　ＯＬ　（全４頁）

(21)出願番号　特願平6－263934

(22)出願日　平成６年(1994)10月27日

(71)出願人　000000295
沖電気工業株式会社
東京都港区虎ノ門１丁目７番12号

(72)発明者　岩野　正博
東京都港区虎ノ門１丁目７番12号　沖電気工業株式会社内

(72)発明者　岩崎　様二
愛知県名古屋市中区丸ノ内３丁目22番21号　株式会社沖テック内

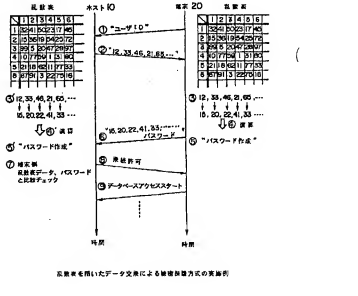
(74)代理人　弁理士　鈴木　敏明

(54)【発明の名称】　乱数表を用いたデータ交換による機密保護方式

(57)【要約】

【目的】　ホストコンピュータへの不法アクセスを防止することが可能な乱数表を用いたデータ交換による機密保護方式を提供すること。

【構成】　端末２０よりホストコンピュータ１０への接続要求を行う際、この端末２０はユーザＩＤをホストコンピュータ１０に送信する。ホストコンピュータ１０がユーザＩＤを受信すると、所定のデータを端末２０に送信するとともに、この所定のデータに基づいて演算処理を行う。一方、端末２０がホストコンピュータ１０から所定のデータを受信すると、このデータに基づいて所定の演算処理を行い、この演算結果を含むデータをパスワードとしてホストコンピュータ１０に送信する。ホストコンピュータ１０は、所定のデータに基づいて演算処理したデータと端末２０より受信したパスワードとを照合し、一致した場合に端末２０からの接続要求を受け入れる。



乱数表を用いたデータ交換による機密保護方式の実施例

1

【特許請求の範囲】
【請求項１】　端末よりホストコンピュータへの接続要求を行う際、この端末はユーザＩＤを前記ホストコンピュータに送信し、
前記ホストコンピュータが前記ユーザＩＤを受信すると所定のデータを前記端末に送信するとともに、前記所定のデータに基づいて演算処理を行い、
前記端末が前記ホストコンピュータから所定のデータを受信すると、このデータに基づいて所定の演算処理を行い、少なくともこの演算結果を含むデータをパスワードとして前記ホストコンピュータに送信し、
前記ホストコンピュータは前記所定のデータに基づいて演算処理したデータと前記端末より受信したパスワードとを照合し、一致した場合に前記端末からの接続要求を受け入れることを特徴とする機密保護方式。
【請求項２】　請求項１に記載の機密保護方式において、前記端末は演算処理した演算結果のデータと予め決めてあるパスワードとを前記端末からのパスワードとして前記ホストコンピュータに送信することを特徴とする機密保護方式。
【請求項３】　請求項１に記載の機密保護方式において、前記演算処理は乱数表を用いて行うことを特徴とする乱数表を用いたデータ交換による機密保護方式。
【請求項４】　請求項３に記載の機密保護方式において、前記ホストコンピュータおよび端末は同一の乱数表を備えることを特徴とするネットワークシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は機密保護方式、より具体的にはコンピュータ間通信を行う際に乱数表などを用いてアクセス権の判定を行う機密保護方式に関する。
【０００２】
【従来の技術】従来、端末からセンターコンピュータ（ホストコンピュータ）のメインデータベースに接続要求が行われた場合、センターコンピュータは端末から送られてきたユーザＩＤおよびパスワードを照合することで当該端末にアクセス権があるか否かの判定を行っている。すなわち、センターコンピュータは、入力したユーザＩＤでユーザを特定し、ユーザ固有のパスワードで各自データの機密保護の解除を行っている。このように、これらユーザＩＤ、パスワードは端末側から一方的に入力され、センターコンピュータで予め登録されたユーザＩＤ、パスワードと比較してアクセス権があるかどうかを決定していた。
【０００３】
【発明が解決しようとする課題】しかしながら、このような従来の方式では、ユーザＩＤは一般に公開されたものであり、またパスワードはユーザ各自固有のものであるが、その実体は２進値の組み合わせである。したがって、コンピュータでランダムに組み合わせれば、簡単にパスワードを見つけ出すことが可能である。このため、ある程度コンピュータの知識があれば、誰でも比較的簡単に他人のデータへアクセスすることが可能であり、悪意によりデータが破壊できるという問題点があった。

2

【０００４】本発明はこのような従来技術の欠点を解消し、ホストコンピュータへの不法アクセスを防止することが可能な乱数表を用いたデータ交換による機密保護方式を提供することを目的とする。
【０００５】
【課題を解決するための手段】本発明は上述の課題を解決するために、ホストコンピュータは接続要求を行った端末に対して所定のデータを送信するとともに、このデータの演算処理を行う機能を備える。ホストコンピュータはまた、この演算処理結果を端末から送られてきたパスワードと照合し、この結果により接続を許可するかどうかの判断を行う。また、アクセス権のある端末は、ホストコンピュータから送られてきた所定のデータをホストコンピュータと同様の演算処理を行う機能を備え、少なくともこの演算処理結果を含むデータを、パスワードとして接続の際にホストコンピュータに送信する機能を備えている。
【０００６】
【作用】本発明によれば、端末よりホストコンピュータへの接続要求を行う際、この端末はユーザＩＤをホストコンピュータに送信する。ホストコンピュータがユーザＩＤを受信すると、所定のデータを端末に送信するとともに、この所定のデータに基づいて演算処理を行う。一方、端末がホストコンピュータから所定のデータを受信すると、このデータに基づいて所定の演算処理を行い、少なくともこの演算結果を含むデータをパスワードとしてホストコンピュータに送信する。ホストコンピュータは、所定のデータに基づいて演算処理したデータと端末より受信したパスワードとを照合し、一致した場合に端末からの接続要求を受け入れる。
【０００７】
【実施例】次に添付図面を参照して本発明による乱数表を用いたデータ交換による機密保護方式の実施例を詳細に説明する。
【０００８】図１は本発明による乱数表を用いたデータ交換による機密保護方式の実施例を示す処理手順であり、図２は本実施例が適用されるネットワークシステムの構成図である。図２において、ネットワーク１００は公衆網などの広域ネットワークまたは社内ＬＡＮのようなローカルエリアネットワークなどの通信ネットワークであり、ホストコンピュータ１０または複数の端末２０、３０が接続されている。
【０００９】ホストコンピュータ１０は、種々のデータが蓄積されているデータベース１２と接続されたコンピュータシステムである。ホストコンピュータ１０は、後述する乱数表を備え、端末からの接続要求があると、こ

の乱数表を用いて接続要求を行った端末にアクセス権があるかどうかを確認する機能を備えている。

【００１０】端末２０および３０は通信機能を備えたたとえばパーソナルコンピュータなどである。なお、ここでは端末２０はホストコンピュータ１０のデータベース１２へのアクセス権のある端末とし、また端末３０はデータベース１２へのアクセス権の無い端末とする。すなわち、端末２０にはホストコンピュータ１０と同一の乱数表を備え、ホストコンピュータ１０に接続要求を行う際にこの乱数表に従って演算処理を行い、これをユーザのパスワードとともにホストコンピュータ１０に送る。

【００１１】次に、図１を用いて端末２０よりホストコンピュータ１０に接続要求を行った場合の処理手順を説明する。端末２０からホストコンピュータ１０のデータベース１２にアクセスする場合、ホストコンピュータ１０と接続後、接続要求として自分のユーザＩＤを送信する（①）。ホストコンピュータ１０は①のユーザＩＤを受信すると、このユーザＩＤが実際に登録されているかどうかを確認し、登録が確認されればあらかじめ決められた範囲内（乱数表選択範囲内）のデータを、システムで決められた個数だけ端末２０に送信する（②）。

【００１２】端末２０は②で送られたきたデータ③を受信すると、乱数表を用いてこのデータの演算処理を行う。具体的には、端末２０が③のデータ"１２，３３，４６，２１，６５，．．．"を受信すると、端末２０はマトリックスを構成している乱数表の"１２（行が１で列が２）"に対応する数値"１５"、"３３"に対応する数値"２０"、"４６"に対応する数値"２２"、"２１"に対応する数値"４１"、"６５"に対応する数値"３３"、．．．を演算処理する（④）。そして、この処理結果にユーザＩＤに対応する自分のパスワードを付加してパスワードを作成し（⑤）、これをホストコンピュータ１０に送る（⑥）。

【００１３】一方、ホストコンピュータ１０は、②で送信したデータ③'を乱数表を用いて端末２０と同様の演算処理を行い（④'）、受信したユーザＩＤに対応するパスワードを付加してパスワードを作成する（⑤'）。ホストコンピュータ１０は、端末２０から受信したパスワード⑤を受信すると、これと作成したパスワード⑤'を照合し、端末２０が正規のユーザであるかどうかを判断する（⑦）。パスワード⑤とパスワード⑤'が一致すれば、ホストコンピュータ１０は端末２０を正規登録ユーザとして接続許可を送信する（⑧）。これにより、端末２０はデータベース１２へのアクセスが可能となる（⑨）。

【００１４】たとえば、データベース１２へのアクセス権の無い端末３０は端末２０のような機密保護機能を備えていない。このため、他人のユーザＩＤを盗用してホストコンピュータ１０にアクセスしても、端末３０は②で送られたきたデータ③を演算処理することができず、実質的にパスワードを見つけ出すことが不可能となり、接続不許可になる。

【００１５】なお、本実施例においてホストコンピュータ１０が端末２０に送るデータの③の桁数を定期的に変更すれば、より安全性の高い機密保護を行うことができる。また、乱数表をホストコンピュータ１０により定期的に変更することにより、乱数表の解析をほとんど不可能にすることで、さらに安全性の高い機密保護を行うようにしてもよい。

【００１６】

【発明の効果】このように本発明によれば、ホストコンピュータなどとの接続時に端末側のユーザＩＤ、パスワードだけで正規の登録ユーザかどうかを判定するのではなく、必ずホストコンピュータから送られてくるデータを基にパスワードを算出するようにした。これにより、ユーザの確認が的確に行え、悪質なハッカーなどによるホストコンピュータへの不法アクセスを防止することができる。

【図面の簡単な説明】

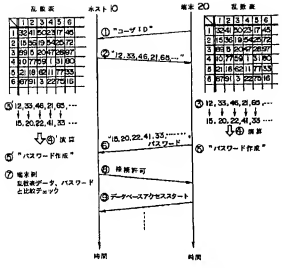
【図１】本発明による乱数表を用いたデータ交換による機密保護方式の実施例を示す説明図である。

【図２】本発明が適用されるネットワークシステムを示したシステム構成図である。

【符号の説明】

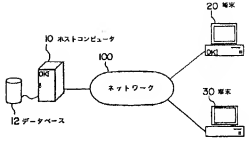
１０　ホストコンピュータ
１２　データベース
２０、３０　端末
１００　ネットワーク

【図1】



乱数表を用いたデータ交換による暗号解読方式の実施例

【図2】



本実施例が適用されるネットワークシステム